Landtag von Baden-Württemberg **Drucksache 17 / 184**

17. Wahlperiode **8.6.2021**

Antrag

der Fraktion der FDP/DVP

und

Stellungnahme

des Ministeriums für Soziales, Gesundheit und Integration

luca-App und Alternativen zur Kontaktnachverfolgung

Antrag

Der Landtag wolle beschließen,

die Landesregierung zu ersuchen,

I. zu berichten,

1. welche potenziellen Sicherheitslücken, die bei Nutzung der Kontaktnachverfolgungsapp „luca“ (im Folgenden „luca-App“) offenbar wurden, ihr vor oder nach dem Erwerb der Lizenzen durch das Land bekannt geworden sind;

2. in welchem Umfang sie, vor und nach dem Erwerb der Lizenzen durch das Land, jeweils die Durchführung einer Sicherheitsüberprüfung, insbesondere von Softwaresicherheitskonzept und Source Code, der luca-App auf potenzielle Schwachstellen veranlasst hat (bitte unter Angabe der konkreten Maßnahmen und jeweiligen Ergebnisse);

3. wie sie die bekannt gewordene Gefahr, dass Angreifer über die luca-App durch sogenannte „Code Injection“ Zugriff auf Daten anderer Nutzer erlangen oder Rechner der Gesundheitsämter durch Ransomware verschlüsseln könnten, bewertet;

4. welche Schlussfolgerungen sie daraus für den zukünftigen Umgang mit der luca-App zieht;

5. wie sie die Möglichkeiten eines Einsatzes der Corona-Warn-App und ihrer Check-In-Funktion allgemein sowie im Bereich der Kontaktnachverfolgung als sinnvolle Alternative zur luca-App bewertet;

Eingegangen: 8.6.2021 / Ausgegeben: 7.7.2021

6. welche Vor- und Nachteile ihrer Ansicht nach der Corona-Warn-App gegenüber der luca-App im Rahmen der Kontaktnachverfolgung jeweils zukommen;

7. aus welchen Gründen sie die Check-In-Funktion der luca-App dem Einsatz der Corona-Warn-App vorzieht;

8. wie sie die tatsächliche Umsetzung der Kontaktnachverfolgung und Identifizierung von mit dem Coronavirus infizierten Menschen beim Einsatz von analogen Adresslisten, einer Datenübermittlung mittels luca-App, der Nutzung der Corona-Warn-App und sonstiger Methoden jeweils (unter gesonderter Darstellung von Dauer, Schnittstellen, Kosten und Fehleranfälligkeit) bewertet;

9. welche weiteren Alternativen zur digitalen Kontaktnachverfolgung sie prüft;

10. aus welchen Gründen die Änderung des § 21 Absatz 8 der Verordnung der Landesregierung über infektionsschützende Maßnahmen gegen die Ausbreitung des Virus SARS-CoV-2 (Corona-Verordnung – CoronaVO), nach der die Verantwortlichen der in § 21 Absatz 1 bis 3, Absatz 5a Nummer 2 genannten Einrichtungen, Betriebe und Veranstaltungen keine Kontaktdaten der Besucher mehr erfassen müssen, erst mit Inkrafttreten am 7. Juni 2021, und damit kurz nachdem die betroffenen Betreiber bereits umfangreiche Maßnahmen zur Kontaktnachverfolgung eingerichtet haben, vorgenommen wurde;

II.

1. über die Cybersicherheitsagentur sicherzustellen, dass die luca-App einer vollständigen Sicherheitsanalyse unterzogen wird, um zu gewährleisten, dass die Infrastruktur der Gesundheitsämter und der dort vorliegenden Daten nicht gefährdet wird;

2. die Verordnung der Landesregierung über infektionsschützende Maßnahmen gegen die Ausbreitung des Virus SARS-CoV-2 (Corona-Verordnung – CoronaVO) vom 13. Mai 2021 dahingehend zu ändern, dass das Erfordernis einer Kontaktdatenerhebung nach § 7 auch durch die Verwendung von pseudonymen digitalen Check-In-Funktionen, wie etwa die der Corona-Warn-App, erfüllt ist.

8.6.2021

Dr. Rülke, Karrais

und Fraktion

Begründung

Es werden immer weitere Sicherheitslücken der luca-App bekannt, die nur langsam und nach Einschätzung von Experten teils nur unzureichend behoben werden (vgl. etwa Internetseite „netzpolitik.org“ vom 26. Mai 2021, Artikel „Schon wieder desaströse Sicherheitslücke in luca App“). Über Schwachstellen in der luca-App sind auch Angriffe auf die Gesundheitsämter nicht mehr auszuschließen. Daher muss die Cybersicherheitsagentur potenziellen Gefahrenquellen, die von „luca“ ausgehen, identifizieren, um zu verhindern, dass die Gesundheitsämter der Gefahr von Cyberangriffen ausgesetzt sind.

Vor dem Hintergrund, dass die deutlich datensparsamere Corona-Warn-App des Bundes mittlerweile ebenfalls über eine Check-In-Funktion verfügt, sollte ihr Einsatz zum Zwecke einer effektiven Kontaktnachverfolgung durch eine entsprechende Änderung der Corona-VO ermöglicht werden.

Stellungnahme

Mit Schreiben vom 1. Juli 2021 Nr. 51-0141.5-017/184 nimmt das Ministerium für Soziales, Gesundheit und Integration im Einvernehmen mit dem Ministerium des Inneren, für Digitalisierung und Kommunen zu dem Antrag wie folgt Stellung:

Der Landtag wolle beschließen,

die Landesregierung zu ersuchen,

I. zu berichten,

1. welche potenziellen Sicherheitslücken, die bei Nutzung der Kontaktnachverfolgungs-app „luca“ (im Folgenden „luca-App“) offenbar wurden, ihr vor oder nach dem Erwerb der Lizenzen durch das Land bekannt geworden sind;

Beim Einsatz des luca-Systems kam es seit seiner Einführung durch bislang insgesamt 13 Länder vereinzelt zum Auftreten von Fehlern oder unerwünschten Eigenschaften. Diese konnten jedoch im Rahmen von Fehlerbehebungen und Weiterentwicklungen durch das verantwortliche Betreiberunternehmen in Zusammenarbeit mit den jeweiligen Beteiligten (Entdecker, Sicherheitsexperten, Auftraggeber und vor allem Gesundheitsämter als Hauptnutzer) schnell beseitigt werden. Dokumentiert sind diese z. B. auf der Blog-Seite von luca (*https://www.luca-app.de/blog/*). Dabei wertet das Ministerium für Soziales, Gesundheit und Integration weder die Diskussion um die zentrale Datenhaltung der mehrfach verschlüsselten Kontaktdaten noch gemachte Fehler bei der Codereferenzierung als mögliche Sicherheitslücke. In die gefragte Kategorie zählen aus Sicht des Ministeriums für Soziales, Gesundheit und Integration bisher:

– das Ausspähen des QR-Code-Schlüsselanhängers und damit die Möglichkeit nach Kopieren des Codes auf die Kontakt-Historie des hinterlegten Codes zuzugreifen, die durch Abschalten der Historienfunktion beseitigt wurde,
– die Möglichkeit zu einer Code-Injection beim Download von CSV-Dateien durch die Gesundheitsämter, die nach Bekanntwerden umgehend beseitigt wurde.

2. in welchem Umfang sie, vor und nach dem Erwerb der Lizenzen durch das Land, jeweils die Durchführung einer Sicherheitsüberprüfung, insbesondere von Softwaresicherheitskonzept und Source Code, der luca-App auf potenzielle Schwachstellen veranlasst hat (bitte unter Angabe der konkreten Maßnahmen und jeweiligen Ergebnisse);

Vor dem Erwerb hat die Landesregierung den Landesbeauftragten für den Datenschutz und die Informationsfreiheit (LfDI) im Rahmen seiner Beratungsfunktion gebeten, zur rechtlichen und technischen Datenschutzkonformität der luca-App Stellung zu nehmen. Der LfDI kam in seiner Stellungnahme zur luca-App vom 2. März 2021 zu folgendem Ergebnis: „Aufgrund der gewonnenen Erkenntnisse empfehlen wir unter dem Blickwinkel des Datenschutzes der Landesregierung, die Nutzung solcher Apps in Baden-Württemberg durch entsprechende Ausstattung der Gesundheitsämter zu ermöglichen, nachdem die Corona-Verordnung des Landes entsprechend angepasst wurde. Die geprüfte App ist aus Sicht des LfDI eine wertvolle Ergänzung der bisherigen staatlichen Schutzmaßnahmen zur Nachverfolgung von Kontakten während der Pandemie. Sie erfüllt die hohen Datenschutz-Standards der DS-GVO. Die Dokumentation der erfolgten Kontakte wird auf technisch höchstem Stand verschlüsselt und es liegt allein in der Hand des luca-Nutzers, ob, wann und mit wem er diese sensiblen Daten teilen möchte. Die ‚luca-App‘ kann einen sehr wertvollen Beitrag leisten, um die Gesundheitsämter bei der Nachverfolgung von Infektionsketten zu entlasten“.

Von Stellen des Bundes wie auch von den Stellen der Länder wurden unterschiedliche Sicherheitsanalysen der luca-App durchgeführt und die Beseitigung der vorgefundenen Schwachstellen beim Hersteller veranlasst. Zur luca-App steht das Ministerium für Soziales, Gesundheit und Integration sowie das Ministerium des Inneren, für Digitalisierung und Kommunen im Austausch mit dem Bund und den anderen Ländern.

3. wie sie die bekannt gewordene Gefahr, dass Angreifer über die luca-App durch sogenannte „Code Injection“ Zugriff auf Daten anderer Nutzer erlangen oder Rechner der Gesundheitsämter durch Ransomware verschlüsseln könnten, bewertet;

Nach dem Bekanntwerden hat das Betreiberunternehmen umgehend reagiert und die für diese Art von Angriff zu diesem Zeitpunkt noch mögliche Lücke geschlossen. Analog zu der Einschätzung des Bundesamts für Sicherheit in der Informationstechnik vom 26. Mai 2021 und des Computer Emergency Response Team Baden-Württemberg wird das Angriffs-Szenario einer Code-Injection über das luca-System abhängig von der konkreten Einsatzumgebung bis zur Behebung als zwar plausibel eingestuft, in der Gesamtsicht mit den zumindest in Baden-Württemberg bei den Gesundheitsämtern verwendeten abgesicherten Systemen aber als beherrschbar bewertet. Es ist zudem kein Fall bekannt, bei dem die Schwachstelle ausgenutzt wurde.

4. welche Schlussfolgerungen sie daraus für den zukünftigen Umgang mit der luca-App zieht;

Das Land Baden-Württemberg hat das luca-System für ein Jahr lizensiert. Das Betreiberunternehmen hat bisher zuverlässig, gut und schnell reagiert und die beauftragte Leistung erbracht. Vor Ablauf der Beauftragung sollen auf Basis der Erfahrungen die künftige Art der Kontaktnachverfolgung sowie die dafür zum Einsatz kommenden Systeme evaluiert werden.

5. wie sie die Möglichkeiten eines Einsatzes der Corona-Warn-App und ihrer Check-In-Funktion allgemein sowie im Bereich der Kontaktnachverfolgung als sinnvolle Alternative zur luca-App bewertet;

Der Einsatz der Corona-Warn-App und deren Check-In-Funktion ist in Baden-Württemberg nicht ausgeschlossen. Durch den Einsatz der Check-In-Funktion der Corona-Warn-App können aber die Vorgaben des § 6 (§ 7a. F.) der Corona-Verordnung nicht erfüllt werden. Dieser verpflichtet insbesondere die Betreiber bestimmter Einrichtungen sowie Veranstalterinnen und Veranstalter dazu, Daten von Anwesenden (Besucherinnen und Besuchern, Nutzerinnen und Nutzern oder Teilnehmerinnen und Teilnehmern) – analog oder digital – zu erheben, damit die Gesundheitsämter im Falle einer Infektion anhand dieser Daten die Kontaktpersonen nachverfolgen können. Um die Voraussetzung für eine möglichst effektive Kontaktpersonennachverfolgung zur Unterbrechung von Infektionsketten durch die Gesundheitsämter zu schaffen, ist es von besonderer Bedeutung, dass die in § 6 (§ 7a. F.) Absatz 1 der Corona-Verordnung ausdrücklich genannten Kontaktdaten der Anwesenden von den hierzu Verpflichteten erhoben und den Gesundheitsämtern zum Zwecke der Auskunftserteilung übermittelt werden können.

Da die Gesundheitsämter nicht an die Corona-Warn-App angebunden werden können und daher eine Datenübermittlung von der Corona-Warn-App an die Gesundheitsämter ausgeschlossen ist, können die Vorgaben des § 6 Absatz 4 (§ 7 Absatz 4a. F.) der Corona-Verordnung durch die Verwendung der Check-In-Funktion der Corona-Warn-App nicht erfüllt werden. Die Check-In-Funktion der Corona-Warn-App zielt vielmehr auf eine anonymisierte Warnung von Teilnehmerinnen und Teilnehmern ab, die sich bei einer Veranstaltung oder beim Besuch einer Einrichtung registrieren. Nach einem Check-In mit der Corona-Warn-App kann daher keine anschließende Kontaktpersonennachverfolgung durch die Gesundheitsämter sichergestellt werden. Die Corona-Warn-App kann natürlich alternativ bzw. parallel zur luca-App in Baden-Württemberg verwendet werden. Durch die alleinige Verwendung der Corona-Warn-App können die Vorgaben des § 6 (§ 7 a. F.) der Corona-Verordnung aber nicht erfüllt werden.

6. welche Vor- und Nachteile ihrer Ansicht nach der Corona-Warn-App gegenüber der luca-App im Rahmen der Kontaktnachverfolgung jeweils zukommen;

Die Corona-Warn-App und das luca-System verfolgen verschiedene Ansätze. Die Corona-Warn-App setzt auf eine anonyme Kontaktprotokollierung über eine zunächst rein technische Anwendung, die mittels Bluetooth Low Energy arbeitet. Damit setzt sie technische Geräte in Form von Mobilfunkgeräten oder künftig spe-

zialisierte Erfassungsgeräte voraus. Wie bereits unter Ziffer 5 dargelegt, kann nach dem derzeitigen Stand der Corona-Verordnung das System der Corona-Warn-App in Baden-Württemberg nicht zur Kontaktnachverfolgung eingesetzt werden, ohne dass dessen Funktionalität erheblich erweitert und gleichzeitig die bisher strikte Anonymisierung aufgehoben wird. Das luca-System ist demgegenüber ein Baustein, um die bestehende Aufgabe der Gesundheitsämter in Baden-Württemberg zur individuellen und persönlichen Kontaktnachverfolgung elektronisch effizient zu unterstützen. Tatsächlich ergeben sich in der Kombination beider Systeme aus Sicht der Landesregierung aber große Chancen für eine wirksame Bewältigung der Pandemie.

7. aus welchen Gründen sie die Check-In-Funktion der luca-App dem Einsatz der Corona-Warn-App vorzieht;

Wie bereits in Ziffer 5 und 6 dargelegt, können durch den Einsatz der Check-In-Funktion der Corona-Warn-App die Vorgaben des § 6 (§ 7 a. F.) der Corona-Verordnung nicht erfüllt werden. Trotzdem ist ein zusätzlicher Einsatz der Corona-Warn-App sinnvoll und empfehlenswert.

8. wie sie die tatsächliche Umsetzung der Kontaktnachverfolgung und Identifizierung von mit dem Coronavirus infizierten Menschen beim Einsatz von analogen Adresslisten, einer Datenübermittlung mittels luca-App, der Nutzung der Corona-Warn-App und sonstiger Methoden jeweils (unter gesonderter Darstellung von Dauer, Schnittstellen, Kosten und Fehleranfälligkeit) bewertet;

Die Gesundheitsämter setzen verschiedene Softwarelösungen zur Kontaktnachverfolgung ein. Die Corona-Warn-App zählt aus den in den Ziffern 5 bis 7 genannten Gründen nicht dazu. Das luca-System bietet den Gesundheitsämtern in ganz Deutschland über ein Benutzungssystem die Möglichkeit, die Kontaktdaten von infizierten Personen und deren Historie über einen bestimmten Zeitraum von 14 Tagen elektronisch zu erhalten. Dazu können die Gesundheitsämter von den Betreiberinnen und Betreibern die passenden Teilnehmerlisten abrufen. Aktuell geht das in drei verschiedenen CSV-Tabellenarten, wobei eine speziell für das bundesweit genutzte SORMAS-System ausgelegt ist.

Der Einsatz von analogen Adresslisten bzw. den sog. „Zetteln“ mit Kontaktdaten wird als ineffizient bewertet und soll daher durch einen möglichst flächendeckenden Einsatz von luca in den Gesundheitsämtern abgelöst werden, mit dem Ziel die sog. „Zettelwirtschaft“ auf ein Minimum zu reduzieren

9. welche weiteren Alternativen zur digitalen Kontaktnachverfolgung sie prüft;

Das Land hat das luca-System nach einem Markterkundungsverfahren beschafft. Vor diesem Hintergrund empfiehlt das Ministerium für Soziales, Gesundheit und Integration die Nutzung von luca. Derzeit werden keine weiteren Alternativen geprüft.

10. aus welchen Gründen die Änderung des § 21 Absatz 8 der Verordnung der Landesregierung über infektionsschützende Maßnahmen gegen die Ausbreitung des Virus SARS-CoV-2 (Corona-Verordnung – CoronaVO), nach der die Verantwortlichen der in § 21 Absatz 1 bis 3, Absatz 5a Nummer 2 genannten Einrichtungen, Betriebe und Veranstaltungen keine Kontaktdaten der Besucher mehr erfassen müssen, erst mit Inkrafttreten am 7. Juni 2021, und damit kurz nachdem die betroffenen Betreiber bereits umfangreiche Maßnahmen zur Kontaktnachverfolgung eingerichtet haben, vorgenommen wurde;

Es ist unzutreffend, dass die Änderung des § 21 Absatz 8 der Corona-Verordnung, die zum 7. Juni 2021 in Kraft getreten ist, die Verantwortlichen der in § 21 Absätze 1 bis 3, Absatz 5a Nummer 2 der Corona-Verordnung genannten Einrichtungen von der Pflicht zur Datenverarbeitung im Rahmen der Kontaktnachverfolgung befreit. Die Anpassung des § 21 Absatz 8 der Corona-Verordnung erfolgte aus redaktionellen Gründen und berücksichtigt, dass bereits in den in § 17 Absatz 1 der Corona-Verordnung genannten Einrichtungen die Datenverarbeitung verpflichtend ist. Die dort enthaltene Aufzählung der betroffenen Einrichtungen wurde entsprechend ausgeweitet, sodass eine ausdrückliche Aufnahme in § 21 Absatz 8 der Corona-

Verordnung rechtstechnisch nicht mehr erforderlich war. In gleicher Weise gilt dies für Veranstaltungen, bei denen gemäß § 11 Absatz 1 der Corona-Verordnung die Verantwortlichen zur Datenverarbeitung verpflichtet sind.

Auch mit Inkrafttreten der Neunten Corona-Verordnung vom 25. Juni 21 ist die Datenverarbeitungspflicht für Veranstaltungen und den genannten Einrichtungen in den jeweiligen Spezialregelungen (§§ 8 ff. der Corona-Verordnung) enthalten.

II.

1. über die Cybersicherheitsagentur sicherzustellen, dass die luca-App einer vollständigen Sicherheitsanalyse unterzogen wird, um zu gewährleisten, dass die Infrastruktur der Gesundheitsämter und der dort vorliegenden Daten nicht gefährdet wird;

Für die Einhaltung der Standards ist der Hersteller der luca-App verantwortlich. Für die Überprüfung der Einhaltung der Standards wird auf die Antwort zu Frage I. 2. verwiesen.

Die Gesundheitsämter sind für die Absicherung der in kommunaler Verantwortung betriebenen Infrastruktur verantwortlich. Eine Beratung der Gesundheitsämter durch die Cybersicherheitsagentur über die erforderlichen Sicherheitsmaßnahmen und deren Umsetzung ist zielführender als eine weitergehende Sicherheitsanalyse der luca-App.

2. die Verordnung der Landesregierung über infektionsschützende Maßnahmen gegen die Ausbreitung des Virus SARS-CoV-2 (Corona-Verordnung – CoronaVO) vom 13. Mai 2021 dahingehend zu ändern, dass das Erfordernis einer Kontaktdatenerhebung nach § 7 auch durch die Verwendung von pseudonymen digitalen Check-In-Funktionen, wie etwa die der Corona-Warn-App, erfüllt ist.

Sowohl die Corona-Verordnung vom 13. Mai, als auch die Corona-Verordnung vom 25. Juni 2021 ermöglichen die Nutzung von elektronischen Verfahren zur Kontaktnachverfolgung. Die eingesetzte Lösung muss allerdings für die Gesundheitsämter verarbeitbare Ergebnisse liefern. In Abstimmung mit dem Landesbeauftragten für den Datenschutz und die Informationsfreiheit ist in § 6 Absatz 4 Sätze 1 und 2 (§ 7 Absatz 4 Sätze 1 und 2 a. F.) der Corona-Verordnung die folgende Regelung normiert worden:

„Die Erhebung und Speicherung kann auch in einer für den zur Datenverarbeitung Verpflichteten nicht lesbaren Ende-zu-Ende-verschlüsselten Form nach dem Stand der Technik erfolgen, solange sichergestellt ist, dass das zuständige Gesundheitsamt die Daten im Falle einer Freigabe durch den zur Datenverarbeitung Verpflichteten im Wege einer gesicherten Übermittlung in einer für das Gesundheitsamt lesbaren Form erhält. Die Ende-zu-Ende-verschlüsselte Form muss die Übermittlung der Daten an das Gesundheitsamt für einen Zeitraum von vier Wochen ermöglichen.“

Dadurch kann die Verwendung von elektronischen Verfahren zur Kontaktnachverfolgung, die die Daten der Personen pseudonymisieren, zulässig sein. Allerdings muss das jeweilige Gesundheitsamt im Falle einer konkret vorzunehmenden Kontaktnachverfolgung die Daten in bearbeitbarer Form, in der Regel also in Klartext zur Verfügung gestellt bekommen. Soweit die Corona-Warn-App zukünftig diese Anforderungen sicherstellen kann, wäre die Nutzung möglich.

Lucha

Minister für Soziales,
Gesundheit und Integration